200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. An organization has deployed Microsoft 365 applications to all employees. Considering the shared responsibility model, who is responsible for the accounts and identities relating to these employees? *

- ○ The organization.
  - ✓ **Correct. In the shared responsibility model, the customer organization always has responsibility for their data, including information and data relating to employees, devices, and accounts and identities.**
- ○ Microsoft, the SaaS provider.
  - ✗ **Incorrect. The shared responsibility model shows that Microsoft as the cloud provider is responsible for hardware the applications run on. The cloud customer is responsible for data, including personal data.**
- ○ There's shared responsibility between an organization and Microsoft.

2. Which of the following measures might an organization implement as part of the defense in-depth security methodology? *

- ○ Locating all its servers in a single physical location.
- ○ Multifactor authentication for all users.
  - ✓ **Correct. Multifactor authentication is an example of defense in-depth at the identity and access layer.**
- ○ Ensuring there's no segmentation of your corporate network.

3. The human resources organization wants to ensure that stored employee data is encrypted. Which security mechanism would they use? *

- Hashing.
- Encryption in transit.
- Encryption at rest.

✓ **Correct. Encryption at rest could be part of a security strategy to protect stored employee data.**

4. Which of the following best describes the concept of data sovereignty? *

- There are regulations that govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally.
- Data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.

✓ **Correct. Data sovereignty is the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.**

- Trust no one, verify everything.

✗ **Incorrect. Trust no one, verify everything describes the Zero Trust model. Data sovereignty is the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.**

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. What is a benefit of single sign-on? *

- A central identity provider can be used.

  ✗ **Incorrect. Although a central identity provider can be used by an organization, it isn't a benefit of single sign-on.**

- The user signs in once and can then access many applications or resources.

  ✓ **Correct. With single sign-on, a user signs in once and can then access a number of applications or resources.**

- Passwords always expire after 72 days.

2. Which relationship allows federated services to access resources? *

- Claim relationship.

  ✗ **Incorrect. A claim relationship isn't used to gain access to resources with federated services.**

- Shared access relationship.

- Trust relationship.

  ✓ **Correct. Federated services use a trust relationship to allow access to resources.**

3. Authentication is the process of doing what? *

- Verifying that a user or device is who they say they are.

✓ **Correct. Authentication is the process of verifying that a user or device is who they say they are.**

- ○ The process of tracking user behavior.
- ○ Enabling federated services.

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. A project manager is setting up a new project that includes members from different departments. The project manager wants to ensure that project team members can collaborate and have shared access to a mailbox, calendar, files, and the project's SharePoint site. Which Microsoft Entra feature can the project manager use to accommodate this requirement, without having to involve an administrator? *

- ○ A managed identity

  ✗ **Incorrect. Managed identities provide an identity for applications to use when connecting to Azure resources and are not designed for collaboration scenarios.**

- ○ A Microsoft 365 group

  ✓ **Correct. A Microsoft 365 group is used for grouping users according to collaboration needs. You can give members of the group access to a shared mailbox, calendar, files SharePoint sites, and more. Because Microsoft 365 groups are intended for collaboration, the default is to allow users to create Microsoft 365 groups, so you don't need an administrator role.**

- ○ A security group

2. An organization has completed a full migration to the cloud and has purchased devices for all its employees. All employees sign in to the device through an organizational account configured in Microsoft Entra ID. Select the option that best describes how these devices are set up in Microsoft Entra ID. *

- ○ These devices are set up as Microsoft Entra ID registered.

✗ **Incorrect. This customer scenario explicitly states that all employees sign in to the device through an organization account and because devices are purchased by the organization, there's no requirement for bring your own device (BYOD). The goal of Microsoft Entra ID registered devices is to provide users with support for BYOD or mobile device scenarios. Microsoft Entra ID registered devices register to Microsoft Entra ID without requiring an organizational account to sign in to the device.**

- ○ These devices are set up as Microsoft Entra ID joined.

✓ **Correct. A Microsoft Entra ID joined device is a device joined to Microsoft Entra ID through an organizational account, which is then used to sign in to the device. Microsoft Entra ID joined devices are generally owned by the organization.**

- ○ These devices are set up as Hybrid Microsoft Entra ID joined.

3. A developer wants an application to connect to Azure resources that support Microsoft Entra authentication, without having to manage any credentials and without incurring any extra cost. Which option best describes the identity type of the application? *

- ○ Service principal

✗ **Incorrect. Service principals are used by applications or services to access Azure resources but application developers must manage and protect the credentials.**

- ○ Managed identity

✓ **Correct. Managed identities are a type of service principal that are automatically managed in Microsoft Entra and eliminate the need for developers to manage credentials.**

- ○ Hybrid identity

Next unit: Summary & resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. After hearing of a breach at a competitor, the security team wants to improve identity security within their organization. What should they implement to provide the greatest protection to user identities? *

- ◯ Multifactor authentication.
  - ✔ **Correct. Multifactor authentication dramatically improves the security of an identity.**
- ◯ Require security questions for all sign-ins.
- ◯ Require strong passwords for all identities.

2. Which of the following additional forms of verification can be used with Microsoft Entra Multifactor Authentication? *

- ◯ Microsoft Authenticator app, SMS, Voice call, FIDO2, and Windows Hello for Business
  - ✔ **Correct. These are all valid forms of verification with multifactor authentication.**
- ◯ Security questions, SMS, Voice call, FIDO2, and Windows Hello for Business
- ◯ Password spray, SMS, Voice call, FIDO2, and Windows Hello for Business

3. A company's IT organization has been asked to find ways to reduce IT costs, without compromising security. Which feature should they consider implementing? *

- ◯ Self-service password reset.

✓ **Correct. Self-service password reset allows users to change or reset their own passwords, thereby reducing the cost of providing administrators and help desk personnel.**

- ○ Biometric sign-in on all devices.
- ○ FIDO2.

✗ **Incorrect. FIDO2 may require the purchase of external keys such as a USB device, which might involve additional expense.**

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. An organization plans to implement Conditional Access. What do admins need to do? *

- ◯ Create policies that enforce organizational rules.

  ✓ **Correct. Conditional Access is implemented using policies that enforce organizational rules.**

- ◯ Check that all users have multi-factor authentication enabled.
- ◯ Amend your apps to allow Conditional Access.

2. Sign-in risk is a signal used by Conditional Access policies to decide whether to grant or deny access. What is sign-in risk? *

- ◯ The probability that the device is owned by the identity owner.

  ✗ **Incorrect. Sign-in risk doesn't calculate any probability relating to users' devices.**

- ◯ The probability that the authentication request isn't authorized by the identity owner.

  ✓ **Correct. Sign-in risk is the real-time calculation that a given authentication request isn't authorized by the identity owner.**

- ◯ The probability that the user is authorized to view data from a particular application.

3. IT admins have been asked to review Microsoft Entra roles assigned to users, to improve organizational security. Which of the following should they implement? *

- ◯ Remove all global admin roles assigned to users.

  ✕ **That's incorrect. There should be the least number of global admin roles required for the organization, and a minimum of two.**

- ◯ Create custom roles.

- ◯ Replace global admin roles with specific Microsoft Entra roles.

  ✓ **That's correct. By following the least privilege security model and assigning specific admin roles, such as billing administrator or user administrator, to more users, instead of global admin roles, organizational security is improved.**

Next unit: Summary & resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. Your organization has implemented important changes in their customer facing web-based applications. You want to ensure that any user who wishes to access these applications agrees to the legal disclaimers. Which Microsoft Entra feature should you implement? *

- ◯ **Entitlement management.**
- ◯ **Microsoft Entra Terms of Use.**
- ◯ **Identity Protection.**

2. An organization is project-oriented with employees often working on more than one project at a time. Which solution is best suited to managing user access to this organization's resources? *

- ◯ **Microsoft Entra Terms of Use.**
- ◯ **Identity Protection.**
- ◯ **Entitlement management.**

3. An organization has recently conducted a security audit and found that four people who have left were still active and assigned global admin roles. The users have now been deleted but the IT organization has been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should they recommend? *

- ◯ **Entitlement management.**
- ◯ **Privileged Identity Management.**
- ◯ **Identity Protection.**

4. Your IT organization recently discovered that several user accounts in the finance department have been compromised. The CTO has asked for a solution to reduce the impact of compromised user accounts. The IT admin team is looking into Microsoft Entra features. Which one should they recommend? *

- ◯ **Identity Protection.**
- ◯ **Conditional Access.**
- ◯ **Entitlement management.**

5. Your IT organization is looking for a solution that provides comprehensive visibility and control over permissions for any identity and any resource in their multi-vendor cloud environment. Which Microsoft solution is best suited to address these needs? *

- ◯ **Identity Protection.**
- ◯ **Privileged Identity Management.**
- ◯ **Permissions Management.**

Check your answers

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. The security admin has created an Azure Network Security Group (NSG) to filter network traffic to a virtual machine. The admin wants to allow inbound traffic using the Remote Desktop Protocol (RDP), but the default NSG rules are currently blocking all inbound traffic that is not from another virtual network or an Azure load balancer. What does the security admin have to do to allow inbound traffic using RDP? *

- ○ Delete the default rule.

  ✗ **Incorrect. The default rules can't be deleted.**

- ○ Create a new network security rule that allows RDP traffic and that has a higher priority than the default rule.

  ✓ **Correct. You can create a new rule to allow RDP that has a higher priority than the default rule**

- ○ There's nothing the admin can do, RDP traffic isn't supported with NSGs.

2. The security admin wants to protect Azure resources from DDoS attacks and needs logging, alerting, and telemetry capabilities. which Azure service can provide these capabilities? *

- ○ Default DDoS infrastructure protection.
- ○ DDoS Network Protection.

  ✓ **Correct. DDoS Network Protection provides the default DDoS infrastructure-level protection plus advanced capabilities, including logging, alerting, and telemetry.**

- ○ Azure Bastion.

3. An organization has several virtual machines in Azure. The security admin wants to deploy Azure Bastion to get secure access to those VMs. What should the admin keep in mind? *

- ◯ Azure Bastion is deployed per virtual network, with support for virtual network peering.

  ✓ **Correct. Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine.**

- ◯ Azure Bastion is deployed per subscription.
- ◯ Azure Bastion is deployed per virtual machine.

4. How can application developers benefit from using Azure Key Vault? *

- ◯ To test and debug their application code.

  ✗ **Incorrect. Application developers can use Azure Key Vault to securely store and retrieve application secrets, such as database connection strings, without having to include it in the application code.**

- ◯ To register their application with Azure
- ◯ To securely store and retrieve application secrets

  ✓ **Correct. Application developers can use Azure Key Vault to securely store and retrieve application secrets, such as database connection strings, without having to include it in the application code.**

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. Microsoft Defender for Cloud covers two broad pillars of cloud security. Which pillar provides visibility to help you understand your current security situation and provides hardening recommendations? *

- ◯ Cloud security posture management (CSPM).

  ✔ **Correct. The CSPM pillar of Microsoft Defender for Cloud provides visibility and to help you understand your current security situation and provides hardening recommendations.**

- ◯ Cloud workload protection (CWP)
- ◯ Microsoft Cloud security benchmark.

2. An organization wants to add vulnerability scanning for its Azure resources to view, investigate, and remediate the findings directly within Microsoft Defender for Cloud. What functionality of Microsoft Defender for Cloud would they need to consider? *

- ◯ Secure score and recommendations functionality that is part of the CSPM pillar of Microsoft Defender for Cloud.

  ✕ **Incorrect. Secure score and recommendations functionality doesn't include vulnerability scanning.**

- ◯ The enhanced functionality that is provided through the Microsoft Defender plans and is part of the CWP pillar of Microsoft Defender for Cloud.

  ✔ **Correct. Microsoft Defender plans provide enhanced security features for your workloads, including vulnerability scanning.**

Security Benchmarks.

3. Your organization wants to improve their security best practices, which option best describes the benefit of using security baselines in Azure? *

Security baselines for Azure apply guidance from the Microsoft cloud security benchmark (or previous benchmarks) to the specific service for which it's defined and provide organizations a consistent experience when securing their environment.

✔ **Correct. Security baselines for Azure apply guidance from the Microsoft cloud security benchmark (or previous benchmarks) to the specific service for which it's defined and provide organizations a consistent experience when securing their environment.**

Security baselines continually assess your resources, subscriptions, and organization for security issues and then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation.

Security baselines in Azure automate the remediation process.

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

1 minute

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. As the lead admin, it's important to convince your team to start using Microsoft Sentinel. You've put together a presentation. What are the four security operation areas of Microsoft Sentinel that cover this area? *

- ○ Collect, Detect, Investigate, and Redirect.

  ✗ **Incorrect. Redirect is not one of the four key aspects of a SIEM/SOAR solution.**

- ○ Collect, Detect, Investigate, and Respond.

  ✓ **Correct. A SIEM/SOAR solution uses collect, detect, investigate, and respond to identify and protect your organization's network perimeter.**

- ○ Collect, Detect, Investigate, and Repair.

2. Your estate has many different data sources where data is stored. Which tool should be used with Microsoft Sentinel to quickly gain insights across your data as soon as a data source is connected? *

- ○ Azure Monitor Workbooks.

  ✓ **Correct. Using the Microsoft Sentinel integration with Azure Monitor Workbooks allows you to monitor data and provides versatility in creating custom workbooks.**

- ○ Playbooks.
- ○ Microsoft 365 Defender.

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft 365 Defender suite is best suited for this purpose? *

- ◯ Microsoft Defender for Office 365.

  ✓ **Correct. Microsoft Defender for Office 365 safeguards against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.**

- ◯ Microsoft Defender for Endpoint.
- ◯ Microsoft Defender for Identity.

2. A cloud access security broker (CASB) provides protection across 4 areas/pillars: visibility to detect all cloud services, data security, threat protection, and compliance. These pillars represent the basis of the Cloud App Security framework upon which Microsoft Defender for Cloud Apps is built. Which pillar is responsible for identifying and controlling sensitive information? *

- ◯ Threat protection.
- ◯ Compliance.

  ✗ **Incorrect. Compliance covers data residency and regulatory compliance.**

- ◯ Data Security.

✓ Correct. Through the Data Security pillar, an admin can identify and control sensitive information and respond to classification labels on content.

3. Which of the following is a cloud-based security solution that identifies, detects, and helps to investigate advanced threats, compromised identities, and malicious insider actions directed at your organization? *

- Microsoft Defender for Office 365
- Microsoft Defender for Identity

✓ Correct. Microsoft Defender for Identity is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

- Microsoft Defender for Cloud Apps

✗ Incorrect. Microsoft Defender for Cloud Apps is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy.

4. Admins in the organization are using the Microsoft 365 Defender portal every day. They want to quickly get an understanding of the organization's current security posture. Which capability in the Microsoft 365 Defender portal will they use? *

- Reports.

✗ That's incorrect. Reports will provide targeted information but doesn't give a snapshot of an organization's security posture.

- Secure Score.

✓ That's correct. Secure Score, in the Microsoft 365 Defender portal, will give a snapshot of an organization’s security posture, and provide details on how to improve it.

- Policies.

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. A new admin has joined the team and needs to be able to access the Microsoft Purview compliance portal. Which of the following roles could the admin use to access the compliance portal? *

- ◯ Compliance Administrator role

  ✓ **Correct. This is one of the multiple roles you can use to access the compliance portal.**

- ◯ Helpdesk Administrator role
- ◯ User Administrator role

2. Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained? *

- ◯ Controls that both external regulators and Microsoft share responsibility for implementing.

  ✗ **Incorrect. External regulators aren't responsible for shared controls. Shared controls are controls that both your organization and Microsoft share responsibility for implementing.**

- ◯ Controls that both your organization and external regulators share responsibility for implementing.
- ◯ Controls that both your organization and Microsoft share responsibility for implementing.

✓ **Correct. Both your organization and Microsoft work together to implement these controls.**

3. A customer has requested a presentation on how the Microsoft Purview compliance portal can help improve their organization's compliance posture. The presentation will need to cover Compliance Manager and compliance score. What is the difference between Compliance Manager and compliance score? *

- ◯ Compliance Manager is an end-to-end solution, in the Microsoft Purview compliance portal, to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

✓ **Correct. Compliance Manager provides admins with the capabilities to understand and improve their compliance score so that they can ultimately improve the organization's compliance posture and help it to stay in line with its compliance requirements.**

- ◯ Compliance Manager is an end-to-end solution, in the Microsoft Purview compliance portal, to enable admins to manage and track compliance activities. Compliance score is a score the organization receives from regulators for successful compliance.
- ◯ Compliance Manager is the regulator who will manage your compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

4 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. Which part of the concept of know your data, protect your data, prevent data loss, and govern your data addresses the need for organizations to automatically retain, delete, store data and records in a compliant manner? *

- ○ Know your data

  ✗ **Incorrect. This component helps to address the need for organizations to understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Instead, govern your data to address the need to automatically retain, delete, store data, and records in a compliant manner.**

- ○ Prevent data loss
- ○ Govern your data

  ✓ **Correct. Capabilities like retention policies, retention labels, and records management enable organizations to govern their data.**

2. As part of a new data loss prevention policy, the compliance admin needs to be able to identify important information such as credit card numbers, across the organization's data. How can the admin address this requirement? *

- ○ Use activity explorer

  ✗ **Incorrect. Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. Instead, use sensitive information types to identify sensitive information like credit card numbers.**

- ○ Use sensitivity labels

- ◯ Use sensitive information types

✓ **Correct. Microsoft provides built-in sensitive information types that you can use to identify data such as credit card numbers.**

3. Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented? *

- ◯ Use the content explorer

✗ **Incorrect. Content explorer enables admins to get a current snapshot of individual items that have been classified across the organization. Instead, use sensitivity labels to help ensure that emails can only be decrypted only by users authorized by the label's encryption settings.**

- ◯ Use sensitivity labels

✓ **Correct. Sensitivity labels help ensure that emails can only be decrypted only by users authorized by the label's encryption settings.**

- ◯ Use records management

4. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement? *

- ◯ Use data loss prevention policies

✓ **Correct. With data loss prevention policies, administrators can now define policies that can prevent users from sharing sensitive information in a Microsoft Teams chat session or Teams channel, whether this information is in a message, or in a file.**

- ◯ Use records management capabilities
- ◯ Use retention policies

5. Due to a certain regulation, your organization must now keep hold of all documents in a specific SharePoint site that contains customer information for five years. How can this requirement be implemented? *

- ◯ Use sensitivity labels

✗ **Incorrect. You don't use sensitivity labels to define data retention. Instead, use retention policies.**

- ○ Use the content explorer
- ○ Use retention policies

✓ **Correct. You can use retention policies to define data retention for all documents in a SharePoint site.**

Next unit: Summary & resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. The compliance admin for the organization wants to explain the importance of insider risk management, to the business leaders. What use case would apply? *

- ○ To identify and protect against risks like an employee sharing confidential information.

✓ **Correct. Use risk management to help protect your organization against these risks.**

- ○ To identify and protect against malicious software across your network, such as ransomware.
- ○ To identify and protect against devices shutting down at critical moments.

✗ **Incorrect. You use insider risk management to protect against risks like an employee sharing confidential information.**

2. To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need? *

- ○ Use Policy Compliance in Microsoft Purview.
- ○ Use Microsoft Purview Communication Compliance.

✓ **Correct. Microsoft Purview Communication Compliance helps minimize communication risks by enabling you to detect, capture, and take remediation actions for inappropriate messages in the organization.**

- ○ Use Microsoft Purview Information Barriers.

✕ **Incorrect. You don't use Microsoft Purview Information Barriers to scan for offensive language. Instead, use Microsoft Purview Communication Compliance.**

3. Your organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need? *

- ○ Use Microsoft Purview Communication Compliance.
- ○ Use activity explorer.
- ◉ Use Microsoft Purview Information Barriers.

✓ **Correct. With Microsoft Purview Information Barriers, you're able to restrict communications among specific groups of users when necessary.**

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. A new admin has joined the compliance team and needs access to eDiscovery (Standard) to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned? *

- ◯ Add them as a member of the eDiscovery Manager role group.

  ✔ **Correct. Members of this role group can create and manage eDiscovery cases. They can also add and remove members, place an eDiscovery hold on users, create and edit searches, and export content from an eDiscovery case.**

- ◯ Add them as a member of the eDiscovery review role.
- ◯ Add them as a member of the eDiscovery custodian role.

2. The compliance admin team needs to be able to collect and copy data into review sets and to be able filter, search, and tag content, which solution can best address their needs? *

- ◯ Audit (Standard).

  ✘ **Incorrect. Audit (Standard) provides with you with the ability to log and search for audited activities and power your forensic, IT, compliance, and legal investigations.**

- ◯ Search
- ◯ eDiscovery (Premium).

  ✔ **Correct. The eDiscovery (Premium) solution allows you to collect and copy data into review sets, where you can filter, search, and tag content so you can**

identify and focus on content that's most relevant.

3. The compliance team wants to obtain intelligent insights to help investigate possible breaches and determine the scope of compromise. Which solution can best address that need? *

- ◯ Audit (Premium).

  ✓ **Correct. Audit (Premium) provides intelligent insights that can help organizations investigate possible breaches and determine the scope of compromise.**

- ◯ Search.
- ◯ eDiscovery (Standard).

  ✗ **Incorrect. The eDiscovery (Standard) lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.**

Next unit: Summary and resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

Knowledge check

2 minutes

Choose the best response for each of the questions below. Then select Check your answers.

Check your knowledge

1. Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization's compliance requirements? *

- ○ Azure Policy
  - ✕ **You can't use Azure Policy to provision resources. Instead, use Azure Blueprints.**
- ○ Azure Rapid Build
- ○ Azure Blueprints
  - ✓ **Azure Blueprint will enable your development teams to define a repeatable set of Azure resources, and achieve shorter development times and faster delivery.**

2. As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use? *

- ○ Use Azure role-based access control (RBAC).
- ○ Use Azure Policy.
  - ✓ **Correct. Azure Policy is used to ensure that your Azure resources comply with your organization's business rules.**
- ○ Use Azure resource locks.

3. Which application in the Microsoft Purview governance portal is used to capture metadata about enterprise data, to identify and classify sensitive data? *

- ○ Data Catalog.
- ○ Data Map.

✔ **Correct. Microsoft Purview Data Map is able to capture metadata about enterprise data, to identify and classify sensitive data.**

○ Data Estate Insights.

Next unit: Summary & resources

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆